

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Patrick Perry (hereinafter "Affiant"), being first duly sworn, hereby deposes and states as follows:

Introduction and Agent Background

1. Affiant is a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement ("ICE") and as such is empowered under the authority of Title 19, United States Code, Section 1598a.

2. Affiant has been the case agent in numerous investigations focusing upon violations of various federal criminal laws, including distribution of child pornography over the Internet and importation and distribution of counterfeit computer parts and components. He also received specialized training in computer forensics. In the course of conducting these investigations, Affiant has executed federal search warrants, seizure and arrest warrants, interviewed witnesses and developed information and expertise using various investigative techniques.

3. This affidavit is made in support of an application for the issuance of a warrant to search the premises known as 57 Madison Road, Wellesley, Massachusetts 02481, more fully described in Attachment A, for the items described in Attachment B, which items constitute contraband, evidence, fruits, and instrumentalities relating to criminal violations of the Digital Millennium Copyright Act, specifically Title 17, United States Code, Sections 1201 and 1204.

4. Title 17, United States Code, Section 1201 (a) provides that:

(1) No person shall circumvent a technological measure that effectively controls access to a work protected under this title...

(2) No person shall manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component, or part thereof, that

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

5. Title 17, United States Code, Section 1201(b) provides that:

(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure

that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

6. Title 17, United States Code, section 1204 provides that:

(a) In General - Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain,

(1) shall be fined not more than \$500,000 or imprisoned for not more than 5 years, or both, for the first offense; and

(2) shall be fined not more than \$1,000,000 or imprisoned for not more than 10 years, or both for any subsequent offense.

7. The facts forth in this affidavit are based upon affiant's personal knowledge, knowledge obtained from other individuals, including federal, state or local law enforcement officers, industry representatives, from a review of documents and Internet websites, communications with others having personal knowledge of events and circumstances described herein, consultations with technical experts in both law enforcement and industry, and information gained through professional training and experience. Because this affidavit is submitted only for the purpose of establishing probable cause to support the issuance of a search warrant, it does not set forth each and every fact learned during the course of the investigation or which is presently

known by law enforcement concerning this investigation.

Video Console Copyright Protection Systems

8. The Microsoft Corporation manufactures and markets digital video game consoles known as the "Xbox" and "Xbox 360." Microsoft also creates and publishes digital Xbox and Xbox 360 video games on optical disc media, and licenses other companies to create and publish Xbox and Xbox 360 video games, which are designed for play on Xbox and Xbox 360 video-game consoles. These video games are protected under the Copyright Act of 1976, Title 17 United States Code, Sections 101, *et seq.*

9. The Sony Corporation manufactures and markets a digital video game console known as the "Playstation." Sony also creates and publishes digital Playstation video games on optical disc media, and licenses other companies to create and publish such games, which are designed for use on Playstation game consoles. These games are protected under the Copyright Act of 1976, Title 17, United States Code, Sections 101, *et seq.*

10. The Nintendo Corporation manufactures and markets a digital video game console known as the "Wii." Nintendo also creates and publishes digital Nintendo video games on optical disk media, and licenses other companies to create and publish such games, which are designed for play on Nintendo Wii video game consoles. These games are protected under the Copyright Act of 1976, Title 17, United States Code, Sections 101, *et seq.*

11. To protect the Xbox, Xbox 360, Playstation and Wii related copyrights and those of the legitimate licensees, Microsoft, Sony and Nintendo each designed digital

copyright protection systems which are integrated into the software code of Xbox, Xbox 360, Playstation and Wii game consoles, and which are integrated into each authentic Xbox, Xbox 360, Playstation and Wii video game optical disc. In simplified terms, the copyright protection systems each include two software designs: Digital Encryption and Authentication Codes.

12. With regards to digital encryption, the software code for every Xbox, Xbox 360, Playstation and Wii game is digitally encrypted according to a specific algorithm, which only Xbox, Xbox 360, Playstation and Wii consoles, respectively, are programmed to decrypt, thereby permitting an authorized user to play video games designed and licensed for each respective system.

13. With regards to the use of authentication codes, every authorized or legitimate Xbox, Xbox 360, Playstation and Wii video game disc contains an authentication code, embedded within the encrypted game code, which is read by the appropriate video console software to verify that the video game in question is an authorized or legitimate version of the game, and it is being run on the appropriate type of game console.

14. The authentication code "hand shake" between the game consoles and the video game discs is intended to prevent such video game consoles from playing unauthorized or pirated reproductions of the encrypted video game code. The encryption of the software code for each video game is intended to prevent the use of alternative game platforms to bypass the authentication / verification process, is also intended to prevent the playing of unauthorized or pirated versions of video games. Together, the encryption of the Xbox, Xbox 360, Playstation and Wii video console

software code and the embedding of an authentication code within legitimate versions of encrypted video game code are intended to prevent standard Xbox, Xbox 360, Playstation and Wii game consoles, or any other type of game platform, from playing unauthorized versions of Xbox, Xbox 360, Playstation and Wii video games on the respective authorized game consoles.

15. Individuals and organizations intending to defeat or "hack" Xbox, Xbox 360, Playstation and Wii copyright protection systems have developed computer chips commonly known as "modification chips" or "modchips" to circumvent the copyright security system employed by the Xbox, Xbox 360, Playstation and Wii game consoles and authorized and licensed Xbox, Xbox, Playstation and Wii video games. These "modchips" contain software code that circumvents the authentication process or "hand shake" between the video game console and authorized or legitimate Xbox, Xbox 360, Playstation and Wii video games. When installed on the main circuit board of a video game console, a "modchip" enables the game console to play authorized versions of video games as well as unauthorized or "pirated" copies of Xbox, Xbox 360, Playstation or Wii games, respectively, stored on unauthorized electronic storage media devices including computer hard drives. Several versions or variations of these "modchips" have been developed and marketed since the introduction of the Microsoft Xbox and Xbox 360, the Sony Playstation and the Nintendo Wii, including, but not limited to the Xecuter, Globe 360, Matrix Infinity and WiiKey modchips.

16. Individuals and organizations intending to defeat or "hack" the copyright protection systems designed into these video game consoles have also developed hardware and software combination devices commonly called "ROMS" which enable

games not designed for Xbox, Xbox 360, Playstation and Wii game consoles to be played on these video game systems. Frequently modified video game consoles will have multiple "ROMS" installed thereby enabling video games designed for multiple Xbox, Xbox 360, Playstation or Wii market competitors to be played on the illegally modified video game console.

17. Individuals and organizations intending to defeat or "hack" the Xbox, Xbox 360, Playstation and Wii copyright protection system will often install large-capacity hard drives (i.e., 200 gigabytes or larger) into a modified video game console designed to work in conjunction with "modification chips." These large capacity hard drives are often pre-loaded with unauthorized or "pirated" copies of video games, and the large-capacity hard drives enable the user of the illegally modified Xbox, Xbox 360, Playstation or Wii game console to copy video games from the optical disc reader in the game console directly to the hard drive for future play without the original optical video game disc. It should be noted that such duplication and/or transfer of such video game code violates the authorized use licenses and conditions of use established by Microsoft for Xbox and Xbox 360 systems and games, as well as the licenses and conditions of use established by Sony for the Playstation and by Nintendo for the Wii video game systems.

Swap Disc Circumvention Devices

18. Individuals and organizations intending to defeat or "hack" the copyright protection system of a Sony Playstation 2 system have developed "swap disks" also known as "boot disks," which are used to circumvent the copyright security system

incorporated into the Playstation 2 console and authorized or licensed Playstation 2 games. A "swap disk" is a CD-ROM that bypasses Sony's verification process when loading a Playstation 2 game, circumventing the technological protection measures built into the console by Sony Computer Entertainment America, Inc., to prevent the playback of pirated and counterfeit games as a means of protecting game publishers' copyrighted material. Once used in a Sony Playstation 2 game console, the "swap disk" enables the console to play both authorized versions of Playstation 2 games and unauthorized or pirated copies stored on optical disks. "Swap disks" are circumvention devices that violate the Digital Millennium Copyright Act ("DMCA"). The most prolific "swap disk" that have been developed and marketed for the Sony Playstation 2 are known as "Swap Magic" discs.

Xbox and Xbox 360 Firmware Flash

19. Individuals and organizations intending to defeat or "hack" the copyright protection system of a Microsoft Xbox or Xbox360 system have also developed something known as a "firmware flashing process," also known as "soft modding." "Firmware flashing" modifies either the Xbox motherboard or the Xbox 360 DVD drive firmware, and circumvents the technological protection measures built into the console by Microsoft Corporation to prevent the playback of unauthorized and pirated content, as a means of protecting game publishers' copyrighted material. Flashing the firmware is accomplished when a user forces unauthorized code into the memory of the Xbox motherboard or the Xbox 360 DVD drive, rewriting its internal BIOS and forcing the system to bypass its usual verification and authentication scheme that ensures the presence of authentic entertainment software. Once used in a Microsoft Xbox or Xbox

360 game console, the rewritten firmware enables the game console to execute and playback both authorized versions of Xbox and Xbox 360 games and unauthorized copies stored on optical discs. Firmware flash circumvention violates the Digital Millennium Copyright Act ("DMCA").

PROBABLE CAUSE

20. In November 2006, Senior Special Agent (SSA) Peter A. Decensi of the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Cleveland, Ohio discovered that the website www.otbmods.com was advertising the sale of illegal modification chips for the Sony Playstation 2, Microsoft Xbox and the Nintendo GameCube gaming consoles. The website also advertised "modification chip" installation services and "pre-modified" gaming consoles with the modification chip already installed.

21. The www.otbmods.com website is a commercial site. When purchasing item(s) customers must place selections in a "shopping cart" and perform a "check out" function to place an order. After placing an order an invoice is provided listing the items sold, cost and price of shipping. The www.otbmods.com website accepts major credit cards (Visa, MasterCard, Discover and American Express) and checks/money orders for payment.

22. A recent notice on the OTB Mods.com website dated May 20, 2007, stated: "We just moved our offices from CO to MA; everything will be back up and running smoothly tomorrow. Sorry for the shipping delay for anyone who placed an order late last week!" (Sic)

23. SSA Decensi discovered that an individual using the screen name of

"Appleguru" was advertising www.otbmods.com business services on the www.Xbox-scene.com and psx-scene.com forum boards. The www.xbox-scene.com forum board is a platform for individuals to discuss topics relating to the Microsoft Xbox gaming console while the psx-scene.com forum board involves the Sony Playstation 2, Playstation 3 and Nintendo Wii gaming consoles. Both forum boards have numerous topics involving hacking and illegally modifying gaming consoles. The following posts were recently discovered on the forum board regarding the sale of illegal modification chips and modification chip installation services of www.otbmods.com:

April 18, 2007 – Psx-scene "OTB Mods – Chips, accessories, premods, parts. We already have a relatively well established customer base and are just starting to expand into the ps2 and gamecube markets (And now Xbox 360, NDS, and Wii too!). Go check out our site over at www.otbmods.com. We also do premods and installations for all systems (Xbox 360, PS2, Gamecube, Wii) interested feel free to shoot me a PM and/or an email at appleguru@otbmods.com) Let me know what you guys think, and leave any feedback on the website/your experience(s) with us here. Thanks." (sic)

May 26, 2005 – Xbox-Scene "I am currently located in MA USA. I can do installs through the mail. I also do repair. I do wii, xbox, xbox 360, gamecube, and ps2 chip installs and firmware flashing. I have a plethora of parts on hand (chips, dvd drives, motherboards, cases, cable, etc) and can fix almost any problem. PM me here, email me: appleguru@appsolutions.com, or chat with me on AIM (iwant2bskiing). The post was updated on May 21, 2007." (sic)

24. A "Whois" search of the domain name "otbmods.com" indicated that the Internet Protocol address is 69.50.192.149. The Internet Protocol address resolves back to a hosting site of Atjeu Publishing, Glendale, Arizona. The registrant for the domain name is Adam Urban, 57 Madison Road, Wellesley, Massachusetts 02481. The administrative and technical contact is also Adam Urban, 57 Madison Road, Wellesley, Massachusetts 02481. Urban provided the e-mail address of appleguru@applesolutions.com on the registration. The domain name was registered

on April 22, 2005, and expires on April 22, 2012.

25. An Accurant Law Enforcement inquiry indicated that Adam S. Urban is associated with the addresses of 57 Madison Road, Wellesley, Massachusetts 02481, and with 902 N. Cascade Avenue, Colorado Springs, Colorado 80946.

26. On January 4, 2007, SSA Decensi, acting in an undercover capacity from Cleveland, Ohio, sent an e-mail to sales@otbmods.com inquiring if the Xecuter 2.6CE and Duo 2SE modification chips were in stock. SSA Decensi also asked if checks or money orders were accepted as payment. The following day, SSA Decensi received a response from Adam@OTB Mods stating that both chips were in stock and that money orders and check were accepted.

27. On January 8, 2007, SSA Decensi visited the website www.otbmods.com and ordered five (5) DuoX2 GS modification chips and (1) Xecuter 2.6CE chip. The cost for the modification chips was \$122.97, including shipping and handling. During the order confirmation portion of the checkout, SSA Decensi was instructed to make the check/money order payable to "OTB Mods" and to mail payment to "OTB Mods, 57 Madison Rd., Wellesley, MA 02481 USA."

28. On January 12, 2007, SSA Decensi obtained a Chase Bank money order in the amount of \$122.97 made payable to "OTB Mods." On the same date, the money order was mailed to OTB Mods, 57 Madison Road, Wellesley, Massachusetts 02481.

29. Financial records obtained from Bank of America NA revealed that the Chase Bank money order in the amount of \$122.97 was deposited into the personal checking account of Adam S. Urban on or about February 1, 2007. An analysis of the deposits in Urban's personal checking account revealed numerous credit card deposits

in the name of OTB Mods. The address shown on the monthly statement as of March 2007, was Adam Urban, 902 N. Cascade Avenue, #283, Colorado Springs, Colorado 80946-3200.

30. On February 2, 2007, SSA Decensi received five (5) DuoX2 GS modification chips and one (1) Xecuter 2.6CE chip via U.S. Postal Service Priority Mail at an undercover mail box in Strongsville, Ohio. The package listed the return address of "OTB Mods, C/O Adam Urban, 902 North Cascade Ave. WB #283, Colorado Springs, CO 80946-0283." The enclosed invoice listed "OTB Mods, 57 Madison Rd., Wellesley, MA 02481 USA."

31. On April 26, 2007, Senior Special Agent (SSA) Robert Berton, ICE, Colorado Springs, Colorado, verified that the address of 902 North Cascade Avenue, #283, Colorado Springs, Colorado, is a mail box located on the campus of Colorado College. An inquiry by SSA Berton with Colorado College indicated that Adam Urban was registered as a student at Colorado College during the spring 2007 semester.

32. On May 24, 2007, Jake Snyder, Manager of Internet Enforcement, Entertainment Software Association (ESA) examined the DuoX2 GS and Xecuter 2.6CE modification chips purchased from www.otbmods.com. The ESA is authorized to conduct examinations on behalf of its member companies, such as Sony Corporation of America, Microsoft Corporation and Nintendo of America Inc.

33. The ESA is an organization based in Washington D.C. that is dedicated to serving the business and public affairs needs of companies that publish video and computer games for game consoles, personal computers, and the Internet. ESA members account for over 90 percent of the \$7.4 billion in entertainment software sold

in the U.S. in 2006 and billions more in export sales of U.S. made entertainment software. The ESA offers a range of services to software publishers including a global anti-piracy program, business and consumer research, government relations and intellectual property rights protection efforts. The ESA represents member companies in the video and computer gaming industry including Sony Computer Entertainment America, Microsoft Corporation, Nintendo and numerous others.

34. Mr. Snyder identified the devices purchased from www.otbmods.com as aftermarket chips known as "modchips." The Duo X2 GS and Xecuter 2.6CE modification chips are illegal circumvention devices designed for the Microsoft Xbox video game console. The DuoX 2 and Xecuter 2.6CE modification chips are small, semiconductor chips that are soldered onto the motherboard of an Xbox console. Once installed, the "modchip" overrides the console's internal BIOS code, circumventing the technological protection measures built into the console by Microsoft Corporation to prevent the playback of unauthorized, pirated or counterfeit games, thus protecting game publisher's copyrighted material. Modification chips and installation of modification chips are circumvention devices and/or acts that violate the Digital Millennium Copyright Act of 1998 (DMCA).

35. On June 7, 2007, SSA Decensi sent an e-mail to sales@otbmods.com inquiring if the Duo X2 and WiiKey modification chips were in stock. SSA Decensi also inquired if money orders were accepted as payment. On the same date, SSA Decensi received a response from Adam@OTB Mods indicating that both chips were in stock and that money orders were accepted.

36. On June 8, 2007, SSA Decensi visited the website www.otbmods.com and

ordered five (5) DuoX2 GS modification chips and three (3) WiiKey modification chips. The cost for the modification chips was \$168.11, including shipping and handling. The order confirmation form produced during the transaction instructed that money orders should be made payable to "OTB Mods" and to mail payments to: "OTB Mods, 57 Madison Rd., Wellesley, MA 02481 USA."

37. On June 12, 2007, SSA Decensi sent an e-mail to sales@otbmods.com verifying the location to send the money order for the modification chips. On the same date, Adam@OTB Mods responded with an e-mail instructing SSA Decensi to send the money order to "OTB Mods, 57 Madison Rd, Wellesley, MA 02481."

38. On June 15, 2007, SSA Decensi obtained a Chase Bank money order in the amount of \$168.11 made payable to "OTB Mods." On the same date, the money order was mailed to OTB Mods, 57 Madison Road, Wellesley, Massachusetts 02481.

39. On June 25, 2007, SSA Decensi received five (5) DuoX2 GS modification chips and three (3) WiiKey modification chip via U.S. Postal Service Priority Mail at an undercover mail box in Strongsville, Ohio. The package listed the return address of "OTB Mods, 57 Madison Rd., Wellesley, MA. 02481 USA." The enclosed invoice also indicated "OTB Mods, 57 Madison Rd., Wellesley, MA 02481 USA."

40. On July 13, 2007, Jake Snyder, Manager of Internet Enforcement for ESA, examined the five (5) DuoX2 GS and the three (3) WiiKey modification chips purchased from www.otbmods.com. Mr. Snyder identified the DuoX2 GS modification chips as illegal circumvention devices for the Microsoft Xbox game console, and the three (3) WiiKey modification chips as illegal circumvention devices for Nintendo Wii gaming console.

41. On July 16, 2007, SSA Decensi again reviewed the www.otbmods.com website. Modification chips advertised for the Sony Playstation 2 included Duo3 Gold modification chip, the Ghost 2 modification chip and the M3 Magic Mushroom modification chip. Modification chips advertised for the Microsoft Xbox included the DuoX2 GS modification chip, the Xecuter 2.6CE modification chip and the Xecuter 3CE modification chip. Modification chips advertised for the Nintendo GameCube included the Duo Q GameCube modification chip, the Qoob Pro modification chip, the Viper GC Extreme modification chip and the Xeno GC V2 modification chip. Modification chips advertised for the Nintendo Wii included the WiiKey modification chip. The website also advertised pre-modified Nintendo GameCube, Sony Playstation 2, Nintendo Wii and Microsoft Xbox gaming consoles. The site also offered modification chip installation service for the Sony Playstation 2, Microsoft Xbox, Nintendo GameCube and Nintendo Wii gaming consoles.

42. As a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), I am familiar with the elements of criminal investigations relating to criminal violations of the Digital Millennium Copyright Act of 1998 (DMCA). Based on my knowledge, training and experience, and that of other Special Agents assisting in the investigation, I know that businesses customarily retain information and records relating to their business and sales transactions, including purchase orders, confirmation letters, correspondence, payment or disbursement ledgers, invoices, employee lists and employment information, employee sales records, customer list, records reflecting contact with customers, supplier list, records reflecting contact with suppliers, bank statements and other financial records, sight drafts,

contracts, vendor correspondence, policies, packing list, sales drafts, inventory lists, air way bills, delivery orders or receipts of delivery, records of payment, and details related to all product sales. Through my experience the above-mentioned information and records are often stored on and generated by the use of computer media or media capable of being read on a computer. In fact the investigation has indicated that that Adam Urban operates a commercial website offering illegal modification chips, modification chip installation services and illegal pre-modified gaming consoles for sale via the Internet. Undercover purchases of the Duo X2, Xecuter 2.6CE and WiiKey modification chips have been made via computer from www.otbmods.com. All of these items, and all of the information however stored, constitute evidence, contraband, fruits, or instrumentalities of violations of Title 17, United States Code, 1201 (a) (2) and (b) and 1204 (a).

43. The terms business "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means created or stored, including any electrical, electronic, magnetic form (such as any information on an electronic or magnetic storage device, including hard drives, floppy diskettes, ZIP disc, CD-ROMs, optical disc, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

44. Computer hardware, software and electronic files are important to a

criminal investigation in two ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, or fruits of crime.

This warrant request permission to search and seize all computer hardware, software, and electronic files on the premises of 57 Madison Road, Wellesley, Massachusetts 02481, that constitute or may be contraband, and that constitute or may be evidence, instrumentalities, or fruits of violations, by Adam Urban, www.otbmods.com and its owners or agents, of offenses involving the DCMA, Title 17, United States Code, Sections 1201 (a) (2) and (b) and 1204 (a). Based on all of the above-mentioned facts, your affiant believes that computer hardware, software, and electronic files on the premises of 57 Madison Road, Wellesley, Massachusetts 02481, are contraband or constitute evidence, instrumentalities or fruits of crime.

45. The aforementioned facts provide evidence of probable cause to believe that www.otbmods.com and its owners and agents, including but not limited to Adam Urban, have trafficked in and have conspired to traffic in a device that circumvents technological measures that (1) effectively control access to a copyrighted work and (2) effectively protect a copyright owner in a copyrighted work, in violation of the DMCA, Title 17, United States Code, Sections 1201 (a)(2) and (b) and 1204(a). Additionally, there is probable cause to believe that evidence, instrumentalities, contraband, and fruits of those violations will be found inside the premises of 57 Madison Road,

Wellesley, Massachusetts 02481, listed above, including but not limited to:

- a. business records and information;
- b. computer hardware, further described in Attachment B; and
- c. computer software, further described in Attachment B; and
- d. modification chips or other electronic circumvention devices; modified Microsoft Xbox consoles, modified Sony Playstation 2 consoles, modified Nintendo gaming consoles further described in Attachment B.

46. Based upon your affiant's knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices. I also know that during the search of the premises it is rarely possible to complete on-site examination of computer equipment and storage devices for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are many types of computer hardware and software in use today and it is rarely possible to transport all the necessary technical manuals and specialized equipment to the search warrant site to conduct a thorough search. In addition, it is also necessary to consult with computer personnel who have specific expertise in the type of computer, software application operating system that is being searched.
- b. The best practices for analysis of computer systems and storage

media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover "hidden", mislabeled, deceptively-named, erased, compressed, encrypted, or password-protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment such as a law enforcement laboratory is typically required to conduct proper analysis.

- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be impractical to search for data during the execution of the physical search of the premises. The hard drives commonly installed in desktop computers are capable of storing millions of pages of text. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all of the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on site.

47. Due to these concerns, your Affiant requests the Court's permission to seize the computer hardware and associated peripherals as discussed below that are believed to contain some or all of the contraband, evidence, instrumentalities or fruits of crime.

48. Based upon your Affiant's knowledge, training and experience, as well as information provided to me by agents and other individuals involved in the forensic

examination of computers, your Affiant is aware that searches and seizures of evidence from computers taken from search warrant locations commonly require agents to seize most or all of a computer system's input/output and peripheral devices in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. In those instances where computers are removed from the search location, investigators must seize all the storage devices as well as the central processing unit (CPUs) and applicable keyboards and monitors which are integral part of the processing unit. If after inspecting the input/output devices, system software and pertinent computer-related documentation and these items are no longer required, the materials and equipment will be returned in a reasonable amount of time. Attachment C to the warrant, which more particularly describes the returning of hardware and software determined to be no longer necessary to the retrieval and preservation of electronic evidence, is incorporated here by reference.

Analysis of Electronic Data

49. The analysis of electronically stored data whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include but shall not be limited to, surveying various file directories and files that they contain; examining all the structured, unstructured, deleted, and overwritten data on a particular piece of media; opening or reading the first few pages of such files in order to determine their precise content; scanning storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic key-word searches through all electronic storage areas to determine whether occurrences of language contained in

such storage areas exist that are intimately related to the subject matter of the investigation.

TECHNICAL ASSISTANCE NEEDED IN THE EXECUTION OF THIS SEARCH

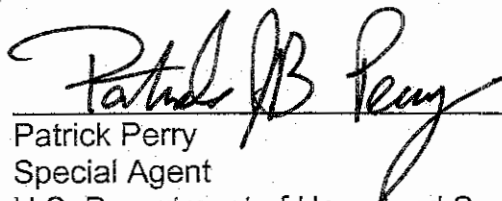
50. In connection with the execution of this search warrant, pursuant to Title 18, U.S.C., Section 3105, Affiant has contacted representatives of Entertainment Software Association, Microsoft, Sony and Nintendo, and has made arrangements to have representatives from one or more of these organizations available by telephone to assist any authorized law enforcement officers in the execution of the search warrant. The representatives will serve only to advise the officer-in-charge of the search location as to technical information and assist in the identification of modification chips, swap disks, illegally modified game consoles and counterfeit or pirated versions of copyright protected products found at the premises to be searched. The officer-in-charge will be responsible for the seizure of any and all evidence.

APPLICATION FOR SEALING ORDER

51. Release of the information contained in this affidavit and related papers is likely to hinder and impede this continuing investigation as well as similar investigations currently being conducted by the Office of Immigration and Customs Enforcement and U.S. Attorney's Offices in various other Districts around the country. Accordingly, it is respectfully requested that this Application, the Affidavit for Search Warrant (including the attachments thereto) and the Search Warrant itself (except for such copies as are necessary for its implementation), be sealed until further Order of the Court so as to not jeopardize these on-going criminal investigations.

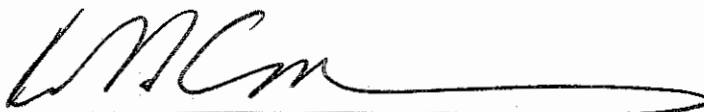
Conclusion

52. Based upon the information set forth above, your Affiant believes that that there is probable cause to believe that the items shown in Attachment B have been used in the commission of a crime and constitute evidence, contraband, fruits, or instrumentalities of violations of Title 17, United States Code, Sections 1201(a) (2) and (b) and 1204 (a) are located at the premises known as 57 Madison Road, Wellesley, Massachusetts 02481, as more fully described in Attachment A.



Patrick Perry
Special Agent
U.S. Department of Homeland Security
Immigration and Customs Enforcement

Sworn to and subscribed before me on this ~~1802-1-8-1111~~ JUL 31 2007 day of July, 2007.



Robert B. Collings
United States Magistrate Judge

HON. ROBERT B. COLLINGS
UNITED STATES MAGISTRATE JUDGE
United States District Court
John Joseph Moakley United States Courthouse
1 Courthouse Way, Suite 7420
Boston, Massachusetts 02210

ATTACHMENT A

Premises To Be Searched

The residence located at 57 Madison Road, Wellesley, MA, further described as a colonial house with the words "Fifty Seven" in black affixed over the front door, located on the right hand side of a cul-de-sac at the end of Madison Road, Wellesley, MA, white/light gray in color, with dark colored shutters, and, as faced from the street, a screened outdoor room to the left side of the house, and a driveway and white garage doors with living area over the garage to the right.

ATTACHMENT B

Items to be seized

1. Any and all "modification chips" or other electronic circumvention devices, including but not limited to the Duo X2, Xecuter 2.6CE and WiiKey modchips; any packaging, documentation or instructions related thereto; and any soldering equipment and other devices or tools used to install modification chips.
2. Any and all business records and information, in whatever form, related to the order, purchase, receipt, sale, manufacture, creation or distribution of Microsoft Xbox consoles, Microsoft Xbox 360 consoles, modified Microsoft Xbox and Xbox 360 consoles, Microsoft video-games, vintage video-games or ROMS; emulators; Sony Playstation consoles, Sony Playstation 2 consoles, Nintendo Wii consoles, Nintendo GameCube consoles, Nintendo video games, modification chips, swap drives, computer hard drives and computer software and programs. Also included in the definition of business records and information are payroll records, employee records, invoices, financial records, bank records, records reflecting assets, records reflecting expenditures, loan records, insurance records, address/telephone records, state & federal tax records, internet service provider records, telephone records, vendor invoices, customer invoices, shipping records, customs records, correspondence including customer or corporate inquiries, complaints or cease and desist orders, records of civil suits or judgements, government filing or correspondence, and government notices.
3. Computer files protected by copyright, including but not limited to software, games and movies.
4. Microsoft Xbox consoles, Microsoft Xbox 360 consoles, modified Microsoft Xbox and Xbox 360 consoles, Xbox video-games, vintage video-games or ROMS, emulators, Sony Playstation consoles, Sony Playstation 2 consoles, modified Sony Playstation and Playstation 2 consoles, Playstation 2 video games, Nintendo Wii consoles, Nintendo GameCube consoles, Nintendo video games, modification chips, computer hard drives, computer software or programs used or installed in any of the foregoing, reference manuals, instructions, packaging, stickers, advertisements and promotional materials related thereto.
5. Computer hardware, meaning any and all computer equipment located on the premises, including any electronic device capable of data processing (such as central processing units, laptop or notebook computers, personal digital assistants, and wireless communications devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media), storage media as defined below, and security devices, also defined below.

6. Computer software, including any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software, including data, data fragments, or control characters integral to the operation of computer software, such as operation systems software, applications software, utility programs, compilers, interpreters, communication software, and other programs used or intended to be used to communicate with computer components.
7. Computer-related documents that explain or illustrate the configuration or use of any seized computer hardware, software, or related items.
8. Data security devices, meaning any devices, programs, or data whether themselves in the nature of hardware or software that can be used to restrict access to, or to facilitate concealment of, any computer hardware, software, computer-related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords, data security hardware (such as encryption devices, chips and circuit boards), data security software or other information (such as test keys and encryption codes), and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.
9. Storage media capable of collecting, storing, maintaining, retrieving, concealing, copying, transmitting, backing-up, and using electronic data, and any devices or instruments, used in the process of imaging, reproducing and distributing copyrighted works. Included within this definition is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed hard disc, external hard disc, removable hard disc, floppy diskettes, compact disc (CDs), digital video disc (DVDs), USB drives, tapes, optical storage devices, laser disc and other memory storage devices.
10. Documents, information, or records, in whatever form, of personal or business activities relating to the operation or ownership of any computer systems, such as usernames, passwords, telephone records, notes, books, diaries, and reference materials.
11. Documents, information, or records, in whatever form, relating to the ownership, occupancy, or use of the premises to be searched, including but not limited to bills, cancelled envelopes, keys, lease agreements and mortgage records.
12. Any and all monetary instruments as they relate to the sale, distribution and installation of illegal circumvention devices in whatever form including but not limited to cash, money orders and bank checks.

ATTACHMENT C

Procedures for Seizing Computers and Related Devices

1. Seizing hardware and software

Agents are authorized to seize and remove from the premises the computer hardware, software, related documentation, and storage media, so that computer analysts can accurately retrieve the items authorized by this warrant in a laboratory or other controlled environment. The retrieval process does not need to be completed within 10 days after the date of the warrant or before the return of the written inventory required by Fed. R. Crim. P. 41(a).

2. Returning hardware and software

If, after inspecting a seized computer system, the agents and computer analysts determine that these items are no longer necessary to retrieve and preserve electronic evidence, the prosecutor determines that they need not be preserved as evidence, fruits or instrumentalities of a crime, and these items do not contain contraband, they should be returned within a reasonable time, upon written request.

If the computer system cannot be returned, agents should, upon written request, make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that are neither the fruits nor instrumentalities of crime nor contraband.